AFRL-IF-RS-TN-2004-3
Final Technical Note
November 2004

QUANTUM INFORMATION PROCESSING

University of California, Berkeley

Sponsored by
Defense Advanced Research Projects Agency
DARPA Order No. K328

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

STINFO FINAL REPORT

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TN-2004-3 has been reviewed and is approved for publication

APPROVED: /s/
DAVID HUGHES
Project Engineer

FOR THE DIRECTOR: /s/
WARREN H. DEBANY, JR.
Technical Director
Information Grid Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	November 2004	**FINAL** **Jan 00 – Dec 03**

4. TITLE AND SUBTITLE

QUANTUM INFORMATION PROCESSING

5. FUNDING NUMBERS

G - F30602-00-2-0601
PE - 62301E
PR - K328
TA - 03
WU - A1

6. AUTHOR(S)

Umesh Vazirani, Christos Papadimitriou, Alistair Sinclair

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

University of California, Berkeley
Sponsored Project Office
336 Sproul Hall
Berkeley CA 94720

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Advanced Research Projects Agency
3701 North Fairfax Drive
Arlington VA 22203-1714

AFRL/IFGC
525 Brooks Road
Rome NY 13441-4505

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

AFRL-IF-RS-TN-2004-3

11. SUPPLEMENTARY NOTES

AFRL Project Engineer: David Hughes/IFGC/(315) 330-4122 David.Hughes@rl.af.mil

12a. DISTRIBUTION / AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 Words)***

This effort supported a Quantum Information Workshop at the University of California, Berkeley. After a cut in funding, the remaining unspent funding was used to support: (1) research related to the internet involving the interplay between mechanism design and computational complexity, (2) improved understanding of the connections between phase transitions in statistical mechanics and mixing times of Markov chain Monte Carlo algorithms, and (3) an investigation of the logic of transcriptional control of various model organisms, with emphasis on characterizing the binding sites of key transcription factors via stochastic models.

14. SUBJECT TERMS

Quantum information, network analysis, Glauber dynamics, mixing times

15. NUMBER OF PAGES 10

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Table of Contents

Revised Statement of Work for Cooperative agreeement F30602-00-2-0601

July 2002

PIs: Richard Karp, Christos Papadimitriou, Alistair Sinclair, Umesh Vazirani

University of California, Berkeley

Context

This revision in the statement of work for Cooperative agreement F30602-00-2-0601 reflects the cut in the funds originally budgeted for year 3 ($250,648). Funds provided in year 2 (for the project "Discrete Models and Algorithms in the Sciences") have been utilized somewhat more slowly than anticipated. This has been due to a long lead-in time for a project with such diverse aims. Nonetheless, the project is now gathering momentum following the highly successful workshop on "Theory of Computation and the Sciences," held in Berkeley in May, 2002, so that current expenditure for year 2 is now over $100,000. Moreover, our plans for faculty and graduate student support, travel and related expenses are more than sufficient to ensure that all the funds allocated for Year 2 of the project (a total of $253,648) will be used by the end of Summer 2003. Below, we list the revised statement of work, and would like to request an extension of the time to expend the remaining funds by a couple of months, until the end of July 2003.

In recognition of the above changed circumstances, the "Scope and Technical Requirements" for Year 3 are revised as follows. We note that the aims of the Quantum Computation portion of the project have already been achieved (as is reflected in the fact that this portion of the funds has been fully expended), and this portion is omitted from Year 3. Moreover, some progress on the goals of the three other themes, as listed below, has already been achieved and is documented in our previous quarterly reports.

Year 2

We expect to deliver a report which will contain the following:

- Various new instances, motivated by study of phenomena related to the Internet, of the emerging interplay between mechanism design and computational complexity.
- Improved understanding of the connections between phase transitions in statistical mechanics models and the mixing times of Markov chain Monte Carlo algorithms.
- An investigation of the logic of transcriptional control in various model organisms, with emphasis on characterizing the binding sites of key transcription factors via stochastic models.

Research funded under DARPA Agreement F30602-00-2-0601

Christos H. Papadimitriou

During the past two years I have been doing research in the interface between ***Theoretical Computer Science, Game Theory***, and ***Networking***. This research was partially supported by the DARPA grant, and was done in collaboration with colleagues Scott Shenker (ICSI and Berkeley), Dick Karp (Berkeley), students Kunal Talwar and Alex Fabrikant, and visitors Muli Shafra (Tel-Aviv University), Vijay Vazirani, and Milena Mihail (Georgia Tech).

The Internet is the first computational artifact that was not designed by a single optimizing entity (except in the most indirect, architectural sense), but emerged from the interaction of various entities, each pursuing its own goals. This fact has two interesting consequences: First, the Internet is the first object of study in the history of Computer Science that must be approached the same way other sciences approach their objects of study (such as the universe, the cell, the brain, the market): with humility, and via observations, measurements, experiments, and the development and validation of falsifiable theories. Second, since the interaction of selfish agents is an important ingredient of the Internet, I am convinced that the mathematical tools needed for its successful study are a novel mix of algorithmic thinking and mathematical economics, especially Game Theory. My work aims at the development of a powerful mathematical methodology, informed by both Theoretical Computer Science and Game Theory, which will be useful in this study. Besides its obvious scientific value as a contribution to the understanding of an intricate and interesting phenomenon, such work, by laying the foundations of a rigorous understanding of the Internet, may be valuable at future junctures, when complex design decisions must be made.

The observation by Faloutsos *et al.* that the Internet topology is scale-free in a rigorous and measurable sense (in that the degrees of the nodes obey a power law) has attracted much attention, and has transformed the practice of Internet protocol simulation. In [1] we extend the work of Carlson and Doyle on "Highly Optimized Tolerance" to show that such scale-free behavior can arise as a result of multi-criterion optimization, in several

contexts. In a related paper [2] we also explain rigorously another, extremely intriguing, observation by Faloutsos *et al.*, namely that the eigenvalues of the Internet topology are also power-law distributed. Much work by others was spawned by these two papers.

In [3] we explore the possibility of Internet routing via incentives to Autonomous Systems to reveal their true routing costs; we show that such incentives can be handled with minimal overhead on top of BGP, the current inter-domain protocol. An experimental observation in [3] that, in the real Internet, such incentives would not be excessive (contrary to the worst-case theoretical predictions) was explained in [4], where we show that, indeed, in scalable random graphs similar to the Internet incentives are low in expectation. In the same paper [4] we also establish that Internet-like random graphs have the property of *expansion*; that is, traffic scales linearly with growth (as opposed quadratically, as it would be expected from other models of sparse graphs). This may help explain the current apparent abundance of bandwidth in the Internet's core, and may also help illuminate the important issue of *the Internet's fault tolerance.*

Economic Theory predicts, via the (twice honored by the Nobel prize) *Arrow-Debreu theorem* that the price mechanism is adequate for clearing markets. In [5] and [6] we look at the issue from an algorithmic point of view, and prove complexity results establishing that (1) prices can in fact be computed efficiently in certain cases, and (2) the problem is difficult to solve exactly, but easy to solve approximately, when the goods are indivisible (i.e., they must necessarily come in integer-valued quantities).

The idea, put forward in our proposal, that there is a productive research area in the interface between Game Theory, Networking, and Theoretical Computer Science, has been very influential. There is now a very active field of research in precisely this interface, attracting several dozen of researchers from all three fields. A workshop at Rutgers/DIMACS in 2001 attracted 60 researchers, while the Berkeley 2002 workshop on Algorithmic Approaches to the Sciences contained a very distinguished and well attended session on Game Theory and Mathematical Economics. I am now organizing (with Vijay Vazirani and Marek Karpinski) a week-long workshop at Dagstuhl (Germany) on the subject with over 50 participants (we had to turn away many applicants), where Nobel laureate John Nash will speak. And I was invited to write a paper and a tutorial on the subject for my field's most prestigious conferences [7,8].

[1] Alex Fabrikant, Elias Koutsoupias, Christos H. Papadimitriou "Heuristically Optimized Trade-Offs: A New Paradigm for Power Laws in the Internet," submitted; preliminary version appeared in ICALP 2002.

[2] Milena Mihail, Christos H. Papadimitriou "On the Eigenvalue Power Law," submitted to *SIAM J. on Computing*; preliminary version appeared in RANDOM 2002.

[3] Joan Feigenbaum, Christos H. Papadimitriou, Rahul Sami, Scott Shenker "A BGP-based mechanism for lowest-cost routing" to appear in *Distributed Computation;* preliminary version appeared in PODC 2002.

[4] Milena Mihail, Christos H. Papadimitriou, Amin Saberi "On certain connectivity properties of the Internet," submitted to FOCS 2003.

[5] Xiaotie Deng, Christos H. Papadimitriou, Shmuel Safra "On the complexity of equilibria," to appear in *JCSS;* preliminary version appeared in STOC 2002.

[6] Nikhil R. Devanur, Christos H. Papadimitriou, Amin Saberi, Vijay V. Vazirani "Market Equilibrium via a Primal-Dual-Type Algorithm," submitted; preliminary version appeared in FOCS 2002.

[7] Christos H. Papadimitriou "Game Theory and Mathematical Economics: A Theoretical Computer Scientist's Introduction," FOCS 2001: 4-8 (invited tutorial).

[8] Christos H. Papadimitriou "Algorithms, games, and the internet," STOC 2001 (invited talk).

Report for Cooperative Agreeement F30602-00-2-0601

PI: Alistair Sinclair
University of California, Berkeley
9 July 2003

A main focus in this part of the project is understanding the connections between *phase transitions* in statistical physics models and computational phenomena, notably the mixing time of local Markov chains (or "Glauber dynamics") on the models. These Markov chains are of interest for two reasons: they are the basis of Monte Carlo algorithms, widely used in computational physics to sample from the Gibbs states of the models; and they are a plausible model for the actual evolution of the physical system described by the model.

PI Alistair Sinclair, together with graduate student Dror Weitz and collaborators Martin Dyer of Leeds University, UK, and Eric Vigoda of the University of Chicago, has established a tight connection between phase transitions and mixing times for the wide class of models known as "spin systems" on regular lattices [2]. Specifically, we show that the Glauber dynamics mixes in optimal (i.e., linear) time if and only if the correlations between spins at different sites of the lattice decay exponentially with the distance between the sites. (This decay of spatial correlations, also known as "spatial mixing," corresponds to one of the notions of phase transition used by physicists.) Results similar to this had been known previously, but our approach has the advantage of being purely combinatorial, dispensing with the heavy machinery from functional analysis used in previous versions.

In related work, Dror Weitz has developed a combinatorial version of a classical result in statistical physics known as "Dobrushin's Uniqueness Condition." This is a local form of spatial mixing condition that has been widely used in the study of phase transitions in spin systems. Weitz's work [3] both generalizes the orginal Dobrushin result, and presents a useful "dual" version that is related to the idea of path coupling used in the analysis of Markov chains.

A major open problem in the analysis of Glauber dynamics in physical models concerns the effect of *boundary conditions* on the mixing time. For example, in the classical Ising model of ferromagnetism, the behavior of the dynamics when the system has "free boundaries" (i.e., there are no external constraints) is well understood: above the critical temperature, the mixing time is very fast (linear in n, the size of the system), while below the critical temperature it is extremely slow (exponential in the diameter of the system). But what happens if we place the system in an environment of, e.g., (+)-spins (i.e., if we fix the values of the spins around the outer boundary to be all (+))? Intuitively, the phenomenon that causes the very slow mixing below the critical temperature — namely, the existence of both a (+) and a (−) phase — should now disappear because the (+) boundary breaks the symmetry. We would therefore expect the mixing time to remain fast (at most polynomial) at *all* temperatures. Surprisingly, a rigorous justification for this intuition has eluded the efforts of the research community up to now.

Over the past year Sinclair and Weitz, working with physicist Fabio Martinelli of the University of Rome, have made the first progress on the above problem. We show that, for the Ising model on a regular tree with (+) boundary conditions at the leaves, the mixing time actually remains linear at *all* temperatures. (On a tree, the mixing time with free boundaries does not become exponential below the critical temperature, but rather polynomial with an arbitrarily large exponent.) Moreover, this result continues to hold even in the presence of an external magnetic

field, which brings the tree model rather close to the classical case of the two-dimensional grid. Our techniques also yield a simpler and more general analysis of the high-temperature regime, in which the mixing time is independent of the boundary conditions. The key ingredient in the analysis is yet another spatial mixing condition, but this time one which is particular to the Gibbs measure under consideration. This opens up the possibility that the condition can be satisfied for some boundary conditions but not others at the same temperature. The spatial mixing condition can be used to bound key quantities such as the spectral gap and the log-Sobolev constant, which are intimately connected to the mixing time. This work has been selected for presentation at the upcoming *IEEE FOCS* in October, 2003 [4].

Extending the above work, Martinelli, Sinclair and Weitz have applied their techniques to other spin systems on trees, including models with hard constraints and spin-glass type interactions, such as the antiferromagnetic Potts model (colorings), the hard-core lattice gas model (independent sets). They have obtained new results on the mixing time of the Glauber dynamics both for arbitrary boundaries and for particular boundary conditions, and related these to phase transitions in the underlying systems. These extensions are reported in a further paper [5].

In continuing joint work with graduate student Steve Chien and former graduate student Lars Rasmussen (now at Digital Fountain, Inc.), Sinclair has been investigating efficient approximation algorithms for the classical problem of computing the permanent of a 0-1 matrix. This is an important problem in statistical physics (as well as several other fields), because of its connection with the partition function of so-called dimer systems. In a paper presented at the 2002 *ACM STOC* Symposium in Montreal [1], Sinclair et al. investigate a novel approach to this problem based on replacing each 1-entry of the matrix by a random basis element of a suitable high-dimensional algebra, and computing the norm-square of the determinant of the resulting matrix. It is easy to see that the resulting output is an unbiased estimator of the permanent; what is remarkable is that the variance decreases very rapidly with the dimension of the algebra. We are optimistic that this result could pave the way to a practical approximation algorithm for this central problem.

Publications

[1] S. Chien, L. Rasmussen and A. Sinclair, "Clifford algebras and approximating the permanent," Proceedings of the 34th Annual ACM Symposium on Theory of Computing, Montreal, Canada, May 2002, pp. 222–231. Expanded version invited to Special Issue of *Journal of Computer & System Sciences*, 2003, to appear.

[2] M. Dyer, A. Sinclair, E. Vigoda and D. Weitz, "Mixing in time and space for lattice spin systems: A combinatorial view," *Proceedings of RANDOM 2002*, Springer Lecture Notes in Computer Science vol. 2483, 2002, pp. 149–163. Expanded version submitted to *Random Structures & Algorithms*.

[3] D. Weitz, "Combinatorial Versions of Dobrushin's Uniqueness Condition," Preprint, 2002.

[4] F. Martinelli, A. Sinclair and D. Weitz, "The Ising model on trees: Boundary conditions and mixing time," to appear in *Proceedings of the 44th IEEE Symposium on Foundations of Computer Science*, October 2003. Preliminary version available at http://www.cs.berkeley.edu/∼dror.

[5] F. Martinelli, A. Sinclair and D. Weitz, "Fast mixing for independent sets, colorings and other models on trees," Preprint, 2003, submitted.